UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/589,593	06/07/2000	Tatsuya Kubota	450108-4457.2	9593

20999 7590 09/22/2004

FROMMER LAWRENCE & HAUG
745 FIFTH AVENUE- 10TH FL.
NEW YORK, NY 10151

EXAMINER	
NGUYEN, MINH DIEU T	
ART UNIT	**PAPER NUMBER**
2137	7

DATE MAILED: 09/22/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/589,593	KUBOTA ET AL.	
	Examiner	Art Unit	
	Minh Dieu Nguyen	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *Amendment dated June 7, 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *12-119* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *12-18,33-38,56,57,68-76,89-97,110 and 111* is/are rejected.

7)☒ Claim(s) *19-32,39-55,58-67,77-88,98-109 and 112-119* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The amendment dated June 7, 2000 has been entered with the cancellation of claims 1-11 and 120-122.

Claims 12-119 are pending.

Priority

2. Applicant cannot rely upon the foreign priority papers to overcome this rejection because a translation of said papers has not been made of record in accordance with 37 CFR 1.55. See MPEP § 201.15.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. **Claims 12, 68-71 and 91-92** are rejected under 35 U.S.C. 102(e) as being anticipated by Wasilewski et al., US 2002/0094084.

a) **As to claims 12, 70 and 92**, Wasilewski discloses a control system for providing secure transmission of interactive information services between a service provider and a customer's set top unit over a digital network comprising: a subscriber management system for managing subscribers' subscriptions for each program or data element (page 1, paragraph [0003,0004]); a subscriber authorization system for generating a scramble key to be used for descrambling the data elements contained in the program for each the data elements (page 2, paragraph [0011]), in this paragraph, Wasilewski discloses the first key used to encrypt the program, this first key is the control word must be transferred to the set top unit to enable the eventual decryption of the program (page 5, paragraph [0047]); and a multiplexer system comprising: an encoding system for encoding each the data elements contained in the program to generate encoded streams consisting of encoded data elements for each program (page 2, paragraph [0010]), it anticipates that digital broadcast system uses MPEG-2 to compress and encode video data and audio data and then broadcasts encoded streams of data over a ground wave or a satellite wave; a multiplexing means for multiplexing the encoded streams generated for each program by the encoding system (Fig. 2D); and a scramble means for selectively scrambling each of the encoded data elements contained in the multiplexed stream based on the scramble key generated by the subscriber authorization system (page 4, paragraph [0046]).

b) **As to claims 68-69 and 71**, their limitations are largely like claims 12 and 70, Wasilewski further discloses a subscriber authorization system for generating a plurality of scramble keys to be used for scrambling a plurality of data elements contained in the program so that a subscriber can watch and/or hear only programs or data elements subscribed for by the subscriber (page 3, paragraph [0036]; pages 4-5, paragraphs [0045-0048]) and a transmission system for transmitting a stream multiplexed by the multiplexer system (Fig. 1, element 20; Figs 2, 2D).

c) **As to claim 91**, Wasilewski discloses a conditional access system for providing a conditional access to only subscribed programs and data elements among a plurality of programs and a plurality of data elements constituting the programs distributed by a program distribution system, the conditional access system comprising: a demultiplexer means for demultiplexing, from the transport stream, a transport stream packet containing a plurality of scrambled data elements constituting the program and for demultiplexing a plurality of enciphered scramble keys associated with the plurality of data elements(Fig. 11, elements 190, 193); a filter means for filtering a transport stream packet containing an enciphered scramble key associated with the programs subscribed for by a subscriber (page 13, paragraph [0130]); a decryption means for deciphering the plurality of enciphered scramble keys; a descramble means for descrambling the plurality of demultiplexed data elements (Fig. 11, element 196) and a decoding means for decoding the plurality of data elements descrambled by the descramble means (page 13, paragraphs [0131-0132]).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. **Claims 13-15** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski et al., US 2002/0094084 in view of Yoshinobu, US Patent 5,699,104.

a) **As to claim 13**, Wasilewski discloses a program distribution system wherein the subscriber management system generates a work key for enciphering the scramble key (page 5, paragraph [0047]) and supplies to the subscriber authorization system a work key as EMM data (page 6, paragraphs [0061-0062]). Wasilewski does not disclose subscriber identification number for identifying the subscriber.

Yoshinobu discloses a broadcasting channel lock system for locking a specific one or more broadcast channels out so that they may not be viewed/received by unauthorized subscribers comprising ID code for identifying subscribers (col. 2, lines 7-12).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of subscriber identification for identify subscribers in the system of Wasilewski, as Yoshinobu teaches so as to have only qualified subscribers accessed the programs/services.

b) **As to claim 14**, Wasilewski discloses a program distribution system wherein the subscriber authorization system comprises a first encryption means for enciphering the work key supplied as the EMM data with a master key to provide an enciphered work key as an output (page 5, paragraph [0048]).

c) **As to claim 15**, Wasilewski discloses a program distribution system wherein the subscriber authorization system supplies to the multiplexer system the enciphered work key enciphered by the first encryption means (see addressed claim 14).

Wasilewski does not disclose the subscriber identification number as enciphered EMM data.

Yoshinobu discloses the subscriber identification number as enciphered EMM data (col. 2, lines 13-19).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of subscriber identification number as enciphered EMM data in the system of Wasilewski, as Yoshinobu teaches so as to have only qualified subscribers accessed the programs/services.

7. **Claims 16-18, 33-38, 56-57, 72-76, 89-90, 93-97 and 110-111** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski et al., US 2002/0094084

in view of Yoshinobu, US Patent 5,699,104 and further in view of Wasilewski, US Patent 5,420,866.

a) **As to claims 16-17, 38, 76 and 97**, Wasilewski (2002/0094084) discloses a program distribution system wherein the subscriber authorization system supplies to the multiplexer system the scramble key as ECM data (page 5, paragraph [0051]). In the prior art 2002/0094084, Wasilewski does disclose the enciphered work key (see addressed claim 14), however Wasilewski and Yoshinobu do not disclose work key identification number for identifying the enciphered work key.

In the reference 5,420,866, Wasilewski discloses a work key table which shows the correspondence between the work key and a work key identification number for identifying the work key (col. 12, lines 12-58).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of work key identification number for identifying the work key and work key table in the system of Wasilewski (2002/0094084) and Yoshinobu, as 5,420,866 teaches so as to easily track keys.

b) **As to claims 18 and 96**, Wasilewski (2002/0094084) discloses a program distribution system wherein the multiplexer system comprises a second encryption means for enciphering the scramble key contained in the ECM data with the work key to provide an enciphered scramble key as an output (page 5, paragraph [0047]).

c) **As to claim 33**, Wasilewski (2002/0094084) discloses a program distribution system wherein the subscriber authorization system comprises a first encryption means for enciphering with a master key a work key used for enciphering the scramble key (pages 4-5, paragraphs [0046-0048]), the subscriber authorization system supplies to the multiplexer system the enciphered work key enciphered by the first encryption means and a subscriber identification number for identifying the subscriber as enciphered EMM data (see addressed claim 15), and the subscriber authorization system supplies to the multiplexer system a work key identification number for identifying the enciphered work key enciphered by the encryption means and the scramble key as ECM data (see addressed claim 16).

d) **As to claims 34, 73 and 94**, Wasilewski (2002/0094084) discloses a program distribution system comprising an encoder/multiplexer control system which generates a program specific information for indicating how to multiplex the plurality of programs, the plurality of data elements constituting the programs, the plurality of ECM data streams and the plurality of EMM data streams and controls the encoder system and the multiplexer system to multiplex the above listed plurality elements (Fig. 1, elements 20, 30; Fig. 2; Figs. 2C-2D; Fig. 12).

e) **As to claims 35, 74 and 95**, Wasilewski (2002/0094084) discloses a program distribution system comprising an encoder/multiplexer control system which generates a program specific information for identifying the packet IDs of a transport

stream packet (page 8, paragraph [0079]), moreover Wasilewski (5,420,866) fully discloses in details such program for identifying the packet IDs of a transport stream packet containing the plurality of data elements constituting the program, a transport stream packet containing the ECM data, a transport stream packet containing the EMM data within a transport stream provided by the data distribution system and which controls the encoder system and the multiplexer system to multiplex the above listed plurality elements (Figs. 3B and 5).

f) **As to claim 36**, Wasilewski (2002/0094084) discloses a program distribution system wherein the encoder system supplies to the multiplexer system the encoded data elements as elementary packets in the form of transport stream packets (Fig. 2D), the subscriber authorization system supplies to the multiplexer system the enciphered EMM data and the ECM data as enciphered EMM packets and ECM packets (page 5, paragraph [0051], page 6, paragraphs [0061-0064]) in the form of transport stream packets respectively and the encoder/multiplexer control system supplies to the multiplexer system the program specific information as PSI packets in the form of transport stream packets.

g) **As to claims 37 and 75**, Wasilewski (2002/0094084) discloses a program distribution system wherein the multiplexer system further comprises, previous to the multiplexing means, a second encryption means for enciphering a scramble key contained in the ECM data (page 5, paragraphs [0047, 0051]).

h) **As to claims 56, 89 and 110**, Wasilewski (2002/0094084) discloses a program distribution system wherein the multiplexer system further comprises a second encryption means for enciphering the scramble keys (page 5, paragraph [0047]) and Wasilewski (5,420,866) further discloses a plurality of buffer means for buffering the PAT packets, the PMT packets, the CAT packets, the transport stream packets containing the data elements, the enciphered EMM packets and the enciphered ECM packets and for providing the transport stream packets to the multiplexing means (Figs 3A, 3B, 4-5).

i) **As to claims 57, 90 and 11**, Wasilewski (2002/0094084) discloses a program distribution system wherein the multiplexer system monitors free area of a plurality of buffers for buffering the transport stream packets containing the data elements and handles buffer overflow issues (Figs. 2C, 2D; page 10, paragraphs [0103-0107]).

j) **As to claims 72 and 93**, see above addressed claims 15-16.

Allowable Subject Matter

8. Claims 19-32, 39-55, 58-67, 77-88, 98-109 and 112-119 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in

independent form including all of the limitations of the base claim and any intervening claims.

The prior arts of Wasilewski (2002/0094084), (5,420,866) and Yoshinobu (5,699,104) do not disclose the work key used by the second encryption means for enciphering the scramble key is not the enciphered work key contained in the EMM data but an unenciphered work key obtained from the work key table supplied by the subscriber authorization system as claimed in claims 19, 39, 77 and 98.

As to any claim not specifically discussed, it is objected to because it depends on one of the claims discussed above.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure

a) US 4,736,421 to Morita et al. discloses system for displaying the subscription state of a pay broadcasting program.

b) US 5,734,589 to Kostreski et al. discloses digital entertainment terminal with channel mapping.

c) US 5,822,324 to Kostreski et al. discloses simulcasting digital video programs for broadcast and interactive services.

d) US 5,825,884 to Zdepski et al. discloses method and apparatus for operating a transactional server in a proprietary database environment.

e) US 6,005,938 to Banker et al. discloses preventing replay attacks on digital information distributed by network service providers.

f) US 6,025,868 to Russo discloses stored program pay-per-play.

g) US 6,067,121 to Shigihara discloses scrambled broadcast system.

h) US 6,069,956 to Kurihara discloses method and apparatus for encrypting multiplexed data streams using key information continued in streams.

i) US 6,188,871 to Kitamura et al. discloses regional common use block of CATV system and CATV system using the regional common use blocks.

j) US 6,424,714 to Wasilewski et al. discloses method and apparatus for providing conditional access in connection-oriented interactive networks with a multiplicity of service providers.

k) US 6,466,671 to Maillard et al. discloses smartcard for use with a receiver of encrypted broadcast signals and receiver.

l) US 2004/0022271 to Fichet et al. discloses signal generation and broadcasting.

m) US 2004/0068541 to Bayassi et al. discloses broadcast and reception and conditional access system therefor.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 703-305-9727. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on 703-306-3036. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Minh Dieu Nguyen
Examiner
Art Unit 2137

mdn
9/3/04

Andrew Caldwell
Andrew Caldwell